CCRS Bit

June 2023

CONTENTS

Cybercrime

- The Metaverse's Darkverse: Potential Ramifications. Link
- Inside Threat Actors: Dark Web Forums vs. Illicit Telegram Communities. Link
- The Great Exodus to Telegram: A Tour of the New Cybercrime Underground. Link
- Asylum Ambuscade: A Cybercrime Group with Espionage Ambitions. Link
- Tracking Diicot: an emerging Romanian threat actor. Link
- MOVEit hack: BBC, BA and Boots among cyber attack victims. Link
- Clop ransomware claims responsibility for MOVEit extortion attacks. Link
- Improved BlackCat Ransomware Strikes with Lightning Speed and Stealthy Tactics. Link
- The BlackCat ransomware gang claims to have hacked the Casepoint legal technology platform used US agencies, including SEC and FBI. Link
- New Horabot campaign takes over victim's Gmail, Outlook accounts. Link
- 'Picture-in-Picture' Obfuscation Spoofs Delta, Kohl's for Credential Harvesting. Link
- New Fast-Developing ThirdEye Infostealer Pries Open System Information. Link
- Malicious Cyber Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes. FBI's Public Service Announcement (PSA). Link

- Researchers discovered spyware, dubbed SpinOk, hidden in 101 Android apps with over 400 million downloads in Google Play. Link
- Anatsa banking Trojan hits UK, US and DACH with new campaign. Link
- Hackers hijack legitimate sites to host credit card stealer scripts. Link
- New Loader Delivering Spyware via Image Steals Cryptocurrency Info. Link
- North Korea’s Lazarus Group Likely Responsible For $35 Million Atomic Crypto Theft. Link
- Elliptic's Typologies Report 2023: Preventing Financial Crime in Cryptoassets. Link
- The Top Ten Latest Crypto Crime Typologies: Pig Butchering. Link
- Mining Pools Are the New Mixers For Cybercriminals: Chainalysis. Link
- Crypto Ponzi Schemes Cost Victims $7.8B in 2022: TRM Labs. Link
- Bitcoin recedes as illicit actors look to Tron, Ethereum, and Binance Smart Chain as blockchain wars evolve. Link
- Crypto hack alarms ramp up as authorities crack down after $3.7 billion stolen. Link
- Hackers make off with $1 million in crypto using Twitter. Link
- Cybercrime Group 'Muddled Libra' Targets BPO Sector with Advanced Social Engineering. Link
- Victims speak out over ‘tsunami’ of fraud on Instagram, Facebook and WhatsApp. Link
- AI Is Being Used to ‘Turbocharge’ Scams. Link
- AI vs. AI: Next front in phishing wars. Link

- Cl0p Cybercrime Gang Delivers Ultimatum after Payroll Breach. Link
- Hackers threaten to leak 80GB of confidential data stolen from Reddit. Link
- Xplain hack impacted the Swiss cantonal police and Fedpol. Link
- The Role of Extraversion in Phishing Victimisation: A Systematic Literature Review. Link
- The Dark Intersection of Online Scams and Human Trafficking. Link
- Thousands of realistic but fake AI child sex images found online, report says. Link
- Sextortionists are making AI nudes from your social media images. Link
- Child predators are using Discord, a popular app among teens, for sextortion and abductions. Link
- Illegal trade in AI child sex abuse images exposed. Link
- Hitting the Books: How hackers turned cybercrime into a commercial service. Link
- Hacked ChatGPT Accounts Are Being Sold On the Dark Web. Link
- INTERPOL issues global warning on human trafficking-fueled. Link
- Fears grow of deepfake ID scams following Progress hack. Link
- The EU Internet Referral Unit (IRU): addressing terrorist content online. Link
- War crimes committed through cyberspace must not escape international justice, says Estonian president. Link
- New Jersey Lawmakers Take Bipartisan Swing at Deepfake Regulation. Link
- US intelligence research agency examines cyber psychology to outwit criminal hackers. Link

- Jailed hacker allowed into IT class, hacks prison computers. Link
- Are the kids alright? How European authorities want to tackle child hacking. Link
- Anonymous Sudan's Attack of European Investment Bank: Money, Politics and PR. Link
- Book: WHY ARE YOU MESSING WITH ME?: Senior Survival Guide on Fraud, Privacy, and Security, by Peter Warmka. Link
- Book: Rinsed, by Geoff White. Link
- Fourth Annual International White Hat Conference. Link
- Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3), Volume X, Year 2023. Link

Digital Investigation and Digital Evidence

- Vidar Malware Using New Tactics to Evade Detection and Anonymize Activities. Link
- Hands-on Ransomware: Exploring Cybercrime. John Hammond's Video. Link
- Dissecting the Dark Web Supply Chain: Stealer Logs in Context. Link
- Policing crypto assets gets an uplift in the UK. Link
- Online gambling enables money laundering – TRACE offers a solution. Link
- The Automated Hunt for Cybergroomers. Link
- Countering violent extremism: Transnational networks for knowledge exchange. Link
- Chainalysis In Action: Israeli Authorities Disrupt Hezbollah and Iran Quds Force Terrorism Financing Crypto Infrastructure, Seize $1.7 Million in First. Link
- Artificial Intelligence to Counter Cyber-Terrorism, by Serena Bianchi et al. Link
- Cybercrime Reporting Mechanisms Vary, and Agencies Face Challenges in Developing Metrics. Link
- Feds seize notorious and shuttered hacking site BreachForums. Link
- Encrypted phone service 'Encrochat' shutdown leads to 6,500 arrests, Europol says. Link
- 2,700 people tricked into working for cybercrime syndicates rescued in Philippines. Link

- US govt offers $10 million bounty for info on Clop ransomware. Link
- RaidForums: The child hacker facing extradition to the US. Link
- Russians charged with hacking Mt. Gox crypto exchange, running BTC-e. Link
- Lead admin of child sex abuse website pleads guilty, faces 20 years to life. Link
- An anti-porn app put him in jail and his family under surveillance. Link
- Twitter Hacker Sentenced to 5 Years in Prison for $120,000 Crypto Scam. Link
- Electronic evidence: new rules to speed up cross-border criminal investigations. To make cross-border investigations more effective, MEPs voted to adopt new rules on the exchange of electronic evidence by law enforcement authorities. Link
- Council adopts EU laws on better access to electronic evidence. Link
- States need to improve criminal asset recovery in combatting money laundering, says MONEYVAL Committee. Link
- Eurojust, Cybercrime Judicial Monitor, issue 8. Link
- Cyclopes Project: 2nd public available annual report for industry and academia. This document contains 3 publicly available reports developed from CYCLOPES practitioners' workshops. These reports outline the priorities of law enforcement at an operational level, and the opportunities for development across the three topics covered by the workshops: Automotive Digital Forensics- organised on 20th - 21st September 2022; Cryptocurrency as a Facilitator for Cybercrime - organised on 7th - 8th December 2022;

Investigations Involving Cloud Services - organised on 22nd - 23rd February 2023. Link

Digital Forensics

- Global Digital Forensics Market Size and Forecast. Link
- Why DFIR Is The New Frontier Of Cybersecurity. Link
- Protect Your Chain Of Custody With Content Hashing And Timestamping. Link
- How Database Forensics Works on New Cybercrime Platforms? Link
- Oxygen Forensics Launches Remote Data Collection Tool, Oxygen Corporate Explorer. Link
- Binalyze introduced Binalyze AIR, the cutting-edge digital forensics software designed to simplify and streamline the investigation process. Link
- Mitre Att&ck Scanning and Mapping Added To DRONE. Link
- Cellebrite Announces Innovative Case-Closing Technology; Raising the Bar for Modern Investigations. Link
- Using Maltego for Combating Crime: Insights from Maltego's NGO Partners. Webinar recording. Link
- MSAB Major Product releases. Link
- Passware Kit Mobile 2023v4 – GPU-Accelerated Unlock Of Samsung S9 and Other Qualcomm-Based Devices. Link
- AutoRecon-XSS - a script designed for automated reconnaissance of XSS vulnerabilities. Link
- Forensia - Anti Forensics Tool for Red Teamers, Used For Erasing Footprints In The Post Exploitation Phase. Link
- RapidDNS/Afuzz - an automated web path fuzzing tool targeted at bug bounty use cases. Link

- CloudFox – a tool for finding exploitable attack paths in cloud infrastructure. Link
- blackarrowsec/redteam-research- a collection of PoC and offensive techniques used by the BlackArrow Red Team. Link
- The Mobile Hacking CheatSheet - a summary of a few interesting basics info regarding tools and commands needed to assess the security of Android and iOS mobile applications. Link
- android-malware-samples - a collection of interesting and diverse Android malware samples. Link
- jsluice – a tool for extracting URLs, paths, and secrets from JavaScript. Link
- DorkGenius – a tool for generating custom dorks for Google, Bing, DuckDuckGo, & more. Link
- Hades - Go Shellcode Loader That Combines Multiple Evasion Techniques. Link
- BishopFox/jsluice, written by TomNomNom, is a Go package and command-line tool for extracting URLs, paths, secrets, and other interesting data from JavaScript source code. Link
- Deepfake Detection and Authenticity Analysis In Amped Authenticate. Webinar recordings. Link
- The Future of Digital Forensics: Trends and Emerging Technologies. Webinar recordings. Link

Digital Surveillance vs. Privacy

- Call for briefing papers for the 2024 edition of the ICRC's Symposium on Cybersecurity and Data Protection, to take place in Luxembourg in January 2024. Link
- Lexisnexis is Selling Your Personal Data to ICE so It Can Try to Predict Crimes. Link
- US intelligence is buying your data – in bulk. Link
- US govt banned NSO's Pegasus, but said to buy rival spyware Paragon Graphite. Link
- US Investors Sniffing Around Blacklisted NSO Group Assets. Link
- Entire Population of Turkey Had Personal Data Exposed Online. Link
- Group-IB Discovers 100K+ Compromised ChatGPT Accounts on Dark Web Marketplaces; Asia-Pacific region tops the list. Link
- Meta Manager Was Hacked With Spyware and Wiretapped in Greece. Link
- Hackers can steal cryptographic keys by video-recording power LEDs 60 feet away. Link
- Apple's security marketing is pushing people away. Link
- Amazon to pay $25m over child privacy violations. Link
- Amazon's Ring doorbell was used to spy on customers, FTC says in privacy case. Link
- A trans-Atlantic comparison of a real struggle: Anonymized, deidentified or aggregated? Link
- Microsoft reserves $425M for LinkedIn GDPR penalty. Link
- TikTok faces EU scrutiny on kids' privacy. Link

- Google forced to postpone Bard chatbot's EU launch over privacy concerns. Link
- TeleSign secretly profiles half of the world's mobile phone users. Link
- LetMeSpy, a phone tracking app spying on thousands, says it was hacked. Link
- ChatGPT Or Google Bard? Privacy or Performance? Outstanding Questions Answered. Link
- CJEU Clarifies the GDPR's Right to Compensation in a judgment in Case C-300/21, UI v Österreichische Post AG clarified individuals' right to compensation for infringement of their rights under GDPR. Link
- The first GDPR fine of the Garante against dark patterns: the importance of legal design. Link
- EU: Final vote on spyware inquiry must lead to stronger regulation. Link
- The EU's Internal Market Committee votes for protecting encryption in the CSA Regulation. Link
- Britain to crack down on unauthorised AI data collection. Link
- Dutch privacy watchdog asks ChatGPT for "clarification" on data. Link
- French Senate votes in favor of public facial recognition pilot. Link
- One of the Last Bastions of Digital Privacy Is Under Threat. Link
- Meet PassGPT, the AI Trained on Millions of Leaked Passwords. Link
- The tech flaw that lets hackers control surveillance cameras. Link

- Science Shouldn’t Give Data Brokers Cover for Stealing Your Privacy. Link
- What GDPR requirements does a company that uses personal information to train an artificial intelligence (AI) need to meet? Link
- IAPP releases AI Governance Professional Body of Knowledge. Link
- The Crucial Role of Antitrust, Anti-Bribery, and Whistleblowers in Personal Data Privacy Frameworks. Link
- Triangulation: Did “the NSA” fail to learn the lessons of NSO? Link
- Launch of Professor Gianclaudio Malgieri's book 'Vulnerability and Data Protection Law'. Link
- Inside the post-Edward Snowden legal challenges, Big Brother Watch Documentary. Link
- Exploring Landmark Privacy Cases with Professor Herke Kranenborg, PrivacyPod Podcast eposide. Link
- Pegasus Spyware: so dangerous that it should be banned? OTW explains... David Bombal’s Podcast episode. Link
- CPDP2023 Session Recordings. Link
- Georgetown Privacy Center will host a three day virtual mini-course entitled No, We Don’t Live In A F%#*ing Simulation. Over Zoom, on August 21, 22, and 23 from 1:00pm-2:30pm ET. Link

Cyber Security

- White House challenges hackers to break top AI models at DEF CON 31. Link
- Millions of PC Motherboards Were Sold With a Firmware Backdoor. Link
- Researchers claim Windows "backdoor" affects hundreds of Gigabyte motherboards. Link
- Million of GitHub Repositories Likely Vulnerable to RepoJacking Attack. Link
- VMware discloses trio of high severity bugs in network monitoring tool. Link
- Malicious Chrome extensions with 75M installs removed from Web Store. Link
- Kaspersky Says New Zero-Day Malware Hit iPhones—Including Its Own. Link
- Dissecting TriangleDB, a Triangulation spyware implant. Link
- Apple patches exploits used in spy campaign 'Operation Triangulation'. Link
- The Security Hole at the Heart of ChatGPT and Bing. Link
- ChatGPT creates mutating malware that evades detection by EDR. Link
- Traditional malware increasingly takes advantage of ChatGPT for attacks. Link
- OWASP lists 10 most critical large language model vulnerabilities. Link
- Quantum hacking alert: Critical vulnerabilities found in quantum key distribution. Link

- Threatening botnets can be created with little code experience, Akamai finds. Link
- U.S. Cybersecurity Agency Adds 6 Flaws to Known Exploited Vulnerabilities Catalog. Link
- CISA adds Progress MOVEit Transfer zero-day to its Known Exploited Vulnerabilities catalog. Link
- US cyber officials offer technical details associated with CL0P ransomware attacks. Link
- CISA orders govt agencies to patch MOVEit bug used for data theft. Link
- Hundreds of federal network devices fail new CISA security requirements. Link
- How to perform an account takeover? A case study of 146 bug bounty reports. Link
- Zyxel Firewalls Hacked by Mirai Botnet. Link
- Mystic Stealer: The New Kid on the Block. Link
- Researchers warn of hackers widely exploiting bug in Zyxel hardware. Link
- Module Installed in Over 100 Android Apps Contained Spyware, Infected Over 421 Million Downloads. Link
- Process Mockingjay: Echoing RWX In Userland To Achieve Code Execution. Link
- New Golang-based Skuld Malware Stealing Discord and Browser Data from Windows PCs. Link
- Stealth Soldier Backdoor Used in Targeted Espionage Attacks in North Africa. Link
- Sneaky DoubleFinger loads GreetingGhoul targeting your cryptocurrency. Link
- Condi DDoS Botnet Spreads via TP-Link's CVE-2023-1389. Link
- Mirai botnet targets 22 flaws in D-Link, Zyxel, Netgear devices. Link

- APT37 hackers deploy new FadeStealer eavesdropping malware. Link
- Hackers Use Weaponized OpenSSH Tool to Hijack Linux Systems. Link
- Fortinet: New FortiOS RCE bug "may have been exploited" in attacks. Link
- Security source code review expert. Shubham Shah. Link
- Fake Security Researcher GitHub Repositories Deliver Malicious Implant. Link
- New Fractureiser malware used CurseForge Minecraft mods to infect Windows, Linux. Link
- New Cryptocurrency Mining Campaign Targets Linux Systems and IoT Devices. Link
- Hackers Use Weaponized PDF Files to Attack Manufacturing, and Healthcare Organizations. Link
- An 8-year vulnerability affecting Bitcoin signing process identified, over 900 addresses affected. Link
- Critical VMware Network Monitoring Tool Flaw under Attack. Link
- US cyber officials offer technical details associated with CL0P ransomware attacks. Link
- RDP honeypot targeted 3.5 million times in brute-force attacks. Link
- Microsoft OneDrive down worldwide following claims of DDoS attacks. Link
- Global hack blamed on Russian cybercriminals affects insurance giant and California pension fund. Link
- Microsoft Uncovers Banking AitM Phishing and BEC Attacks Targeting Financial Giants. Link
- Microsoft links data wiping attacks to new Russian GRU hacking group. Link

- Chinese Hackers Using Never-Before-Seen Tactics for Critical Infrastructure Attacks. Link
- Google claims it caught China government hackers redhanded breaking into hundreds of networks around the world. Link
- Why is it so rare to hear about Western cyber-attacks? Link
- VMware ESXi Zero-Day Used by Chinese Espionage Actor to Perform Privileged Guest Operations on Compromised Hypervisors. Link
- NSA gives guidance on how to protect Windows 10 and 11 machines from the BlackLotus bootkit malware. It's not enough to just patch, the spy agency said. Link
- NSA Releases Guide to Combat Powerful BlackLotus Bootkit Targeting Windows Systems. Link
- WebRTC & IP Address Leak Test Tool to findout if WebRTC is leaking your IP address or if your VPN is working properly by using our leak test tool. Link
- Google Cloud launches Cryptomining Protection Program. Link
- Google announces $20 million investment for cyber clinics. Link
- Apple announces powerful new privacy and security features. Link
- Flipper Zero “Smoking” a Smart Meter is a Bad Look for Hardware Hackers. Link
- New tool scans iPhones for 'Triangulation' malware infection. Link
- Scanner-and-Patcher - A Web Vulnerability Scanner And Patcher. Link
- Progress Software hit with class action lawsuit over MOVEit hack. Link
- Casey Ellis: Pioneering the Bug Bounty Platform to Empower Ethical Hackers. Casey Ellis, the founder of Bugcrowd, is

interviewed by Phillip Wylie, who admires Casey's connection to the hacker community. Link

- Hackers Can Uncover Cryptographic Keys by Recording Footage of Power LEDs. Link
- ENISA AI Cybersecurity Conference. Recordings. Link
- Dark Web & Anonymity Home-Lab. Link